Estonian Health Information System

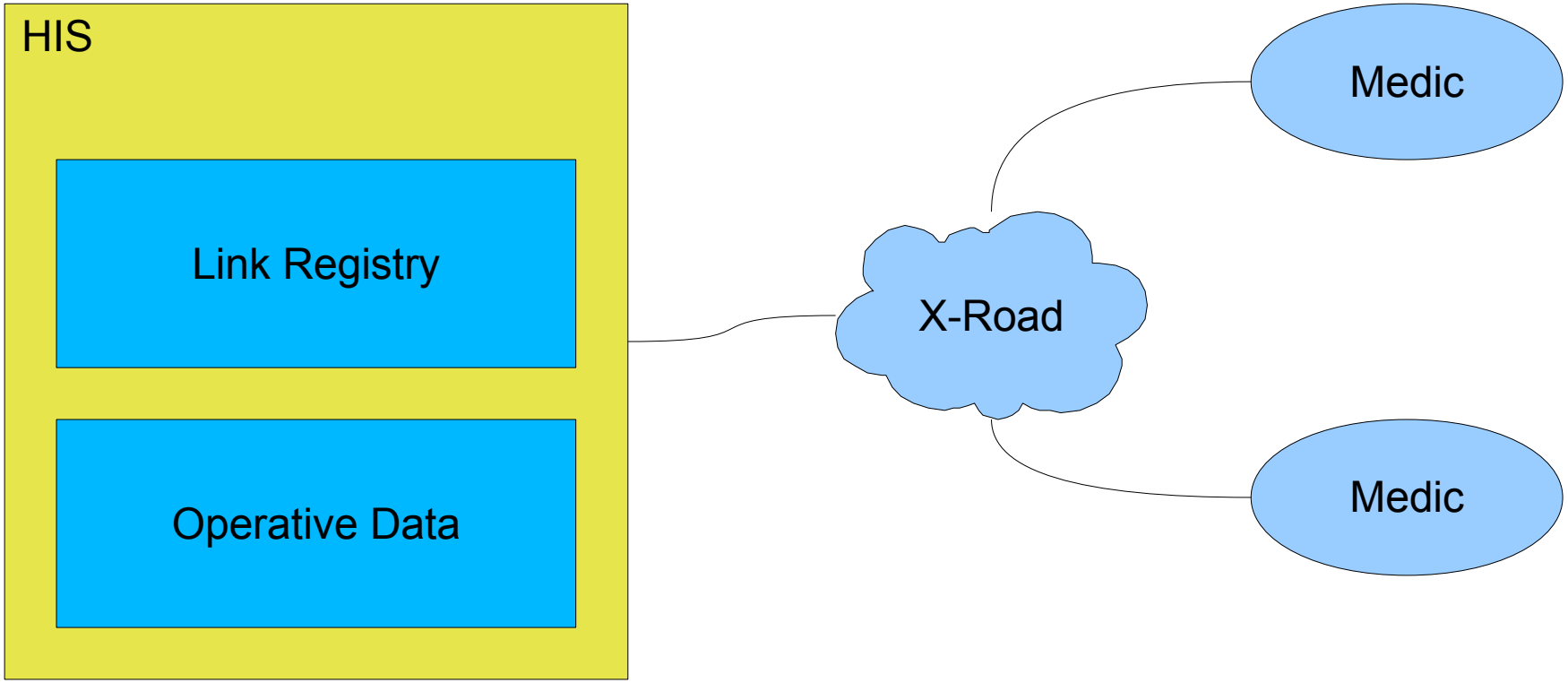
Goals

- Better distribution of health data
  - Doctors can see what other doctors do (better diagnoses)
  - Information about conditions that can affect treatments (allergies etc.)
  - Result: better treatment of patients
- Better medical statistics
  - Especially related to health insurance
- Patients better informed about information about them

However...

- Potential loss of privacy
  - More people can access patient data
  - Potential for big „superdatabase”
- Loss of patient's control over data
- Less accountability/clarity
- Also
  - Money
  - IT-capability of small medical organizations
  - Additional work caused by the system

General Architecture



Participants

- Medical organizations submit data to HIS over X-Road
- X-Road is Estonian governmental middleware that ensures secure transport on messages
- HIS contains link registry that contains metadata about medical records
- Health records are stored in medical institutions, critical data is stored in HIS
- HIS enforces access control policy

Distributed architecture

- Data does not leave medical institution unless necessary
- No party can accumulate much data
- In order to access data, one must first ask for link from centre
- Centre can apply various access control mechanisms

Problems

- Medical institutions must implement online services
- These services have high availability requirements
- Cost + IT capability issues
- **Result:** all data is stored in central HIS, only digital images are linked

Problems (2)

- Problems when developing access control rules
  - Technical problems – how to configure software?
  - Organizational problems – what are the rules?
    - What does it mean for a doctor to be treating a patient?
    - How to handle emergency medicine?
    - Too many exceptions
- **Result:** there are no data-based access control rules

Access control

- Access control is performed by medical institutions that make queries
- Query log analysis is supposed to detect misuses of data

Person's rights

- Person can access HIS over special portal
  - Authentication via ID card
- Person can see his data and query log
- Person can restrict access to data
  - Either to all data or to specific files
  - However, person cannot prevent entering of data into HIS
- Person can give access to other people
  - Delegation also possible

Conclusion

- The system is deployed (2009-01-01) and sort-of works
- Architecture and security measures are compromize between wishes and reality
  - As usual